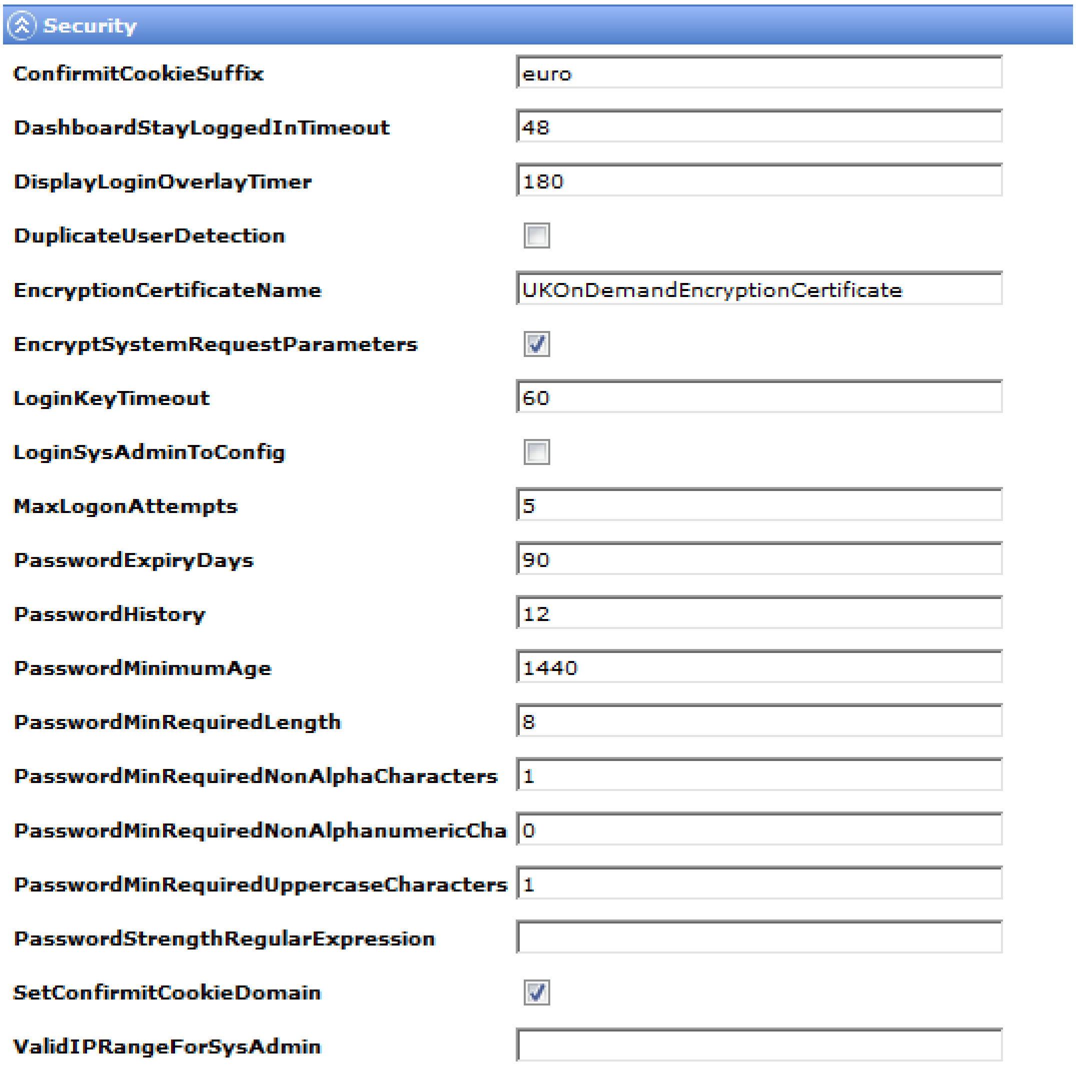
Security in Confirmit Software - SaaS Security

1 System-wide Security Settings in Confirmit Horizons SaaS

The system settings in Confirmit Horizons control many of the configurable built-in security features in the application, for instance timing values for session validity and password restrictions.

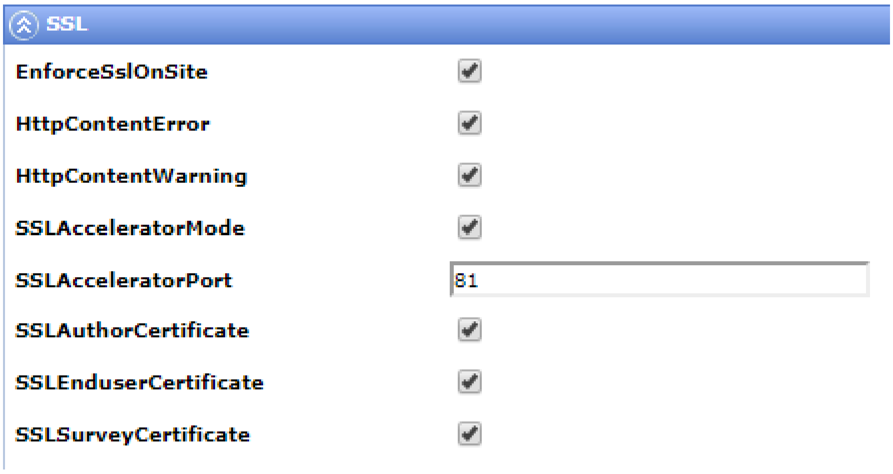


Security

ConfirmitCookieSuffix	euro
DashboardStayLoggedInTimeout	48
DisplayLoginOverlayTimer	180
DuplicateUserDetection	☐
EncryptionCertificateName	UKOnDemandEncryptionCertificate
EncryptSystemRequestParameters	☑
LoginKeyTimeout	60
LoginSysAdminToConfig	☐
MaxLogonAttempts	5
PasswordExpiryDays	90
PasswordHistory	12
PasswordMinimumAge	1440
PasswordMinRequiredLength	8
PasswordMinRequiredNonAlphaCharacters	1
PasswordMinRequiredNonAlphanumericCha	0
PasswordMinRequiredUppercaseCharacters	1
PasswordStrengthRegularExpression	
SetConfirmitCookieDomain	☑
ValidIPRangeForSysAdmin	

2 TLS (SSL) Encryption

Confirmit has purchased SSL certificates for all its web-facing systems, and has enforced HTTPS for Confirmit's Horizons SaaS environments. As HTTPS in enforced, customers with a custom URL for accessing SaaS services must acquire their own SSL certificate for the domain. For On-Premise customers indicating in the system settings that certificates exist for front-end systems, the application will seamlessly redirect users to HTTPS for pages where authentication credentials are exchanged. On-Premise customers also have the option to enforce TSL (SSL) for **all** traffic on their environment. In addition to this Confirmit Horizons also support the HTTP Strict Transport Security response header which can be set on any level in IIS.



SSL

EnforceSslOnSite	☑
HttpContentError	☑
HttpContentWarning	☑
SSLAcceleratorMode	☑
SSLAcceleratorPort	81
SSLAuthorCertificate	☑
SSLEnduserCertificate	☑
SSLSurveyCertificate	☑

3 Backup Encryption

In order to ensure customer data is not accessible outside the controlled Confirmit Horizons servers, we have deployed solutions that encrypt all data before it is backed up to external media. For SQL Server databases, we use the SQL Backup Pro backup software from Red Gate to compress and encrypt backup files even as they are being backed up from the database server (no need to perform post-backup compression or encryption).

For Survey definitions data and launched survey packages we use zip compression and encryption.

All data is encrypted using the AES-256 algorithm. This algorithm is considered extremely secure in the industry and even theoretical methods for brute-forcing an encryption key are not considered computationally feasible.

4 Firewall Protection

Confirmit uses industry-standard firewalls from Cisco and F5 in its Horizons SaaS environments. As with any other network component, our firewalls are configured in an active/passive failover cluster consisting of two identical devices, reducing the time required to recover from a potential hardware failure. This also allows us to perform regular upgrades of device software/firmware without interrupting the availability of the system.

Firewall rulesets are designed to allow only required ports and services to pass through to servers, all other traffic is blocked at the firewall perimeter and silently dropped.

5 Threat Management

In addition to firewalls, we have installed a threat management system from Alert Logic. This consists of a device behind our firewalls which monitors all traffic that is allowed to pass through our network (the network packets are spanned (mirrored) to a secondary port on one of our switches and the original packets are not interrupted).

The network packets are inspected using heuristic methods to analyse the data in packets and match them against known attack patterns. The attack patterns themselves are continuously updated at Alert Logic's Security Operations Center, based on traffic logs from devices that have been placed in some of the most hostile network environments on earth. Attack recognition patterns are then pushed to customers' devices regularly, meaning new types of exploits and attacks can often be recognized before they are regularly used on the Internet.

If the device matches traffic on the network against a known attack vector, it will raise alerts to Alert Logic SOC who will perform a manual analysis and determine whether or not the traffic is part of a potential attack. Based on the findings, they will notify our hosting provider, who will in turn inform Confirmit's Operations team and add firewall blocks as necessary.

6 Security Testing

The Alert Logic Threat Management device also has an additional feature: a built-in vulnerability scanner. Since the device is situated inside the network, behind our firewalls, it can access each host on the network and probe for known vulnerabilities on a host level (missing security updates, expired SSL certificates, standard administrator passwords, and so on). The device will perform a weekly scan of the entire network and sends a report to Confirmit's Operations team with the findings for each scan. We then analyse the findings and plan remediating actions accordingly where this is applicable.

In addition to this, we also regularly commission a third party to perform external vulnerability testing of our environment. In this scenario, a security company will use known attack methods and try to find vulnerabilities by simulating the behaviour of a typical attacker using a variety of methods to find exploits in the system. Results are compiled into a report that is presented to our Operations team. We then plan and implement any changes required to remediate any vulnerabilities, and the third party finally performs a retest to verify whether remediation efforts have been successful. A final report is produced with the updated findings, along with an attestation letter and an executive summary of findings. (We may share the executive summary with customers under NDA upon request).

Similarly, our R&D architecture team regularly commissions vulnerability testing of the Confirmit application from an application perspective, targeting known vulnerabilities in the code (checking for XSS, SQL injection, etc.) as an *authenticated user*. This type of scan allows for a deeper testing of the application itself and ensures that our developers are keeping up to date with current security practices in their code design and execution.

Confirmit Confidential. Copyright © 2019 Confirmit. All Rights Reserved